

Licence professionnelle Réseaux et Sécurité

Projets tuteurs 2013-2014

Sujets proposés à l'Université de Cergy-Pontoise

1. <u>Déploiement d'une architecture téléphonique hybride : PC-Asterisk/PABX analogique + annuaire et proxy (3 élèves)</u>

Tuteur : *Tuyêt Trâm Dang Ngoc*, dntt(à)u-cergy.fr

Le but de ce projet est de déployer la téléphonie sur IP et analogique sur un site puis de l'interconnecter avec un autre site.

a. Site 1

Création d'un autocommutateur analogique

Vous disposez d'un PC contenant les deux cartes suivantes Digium TDM31B TDM PCI Card (3FXS-1FXO). Sur chacune de ces cartes, vous pouvez relier sur les ports FXS, un périphérique analogique FXO (téléphone, fax, etc.) et sur les ports FXO une liaison vers un port FXS.

Le logiciel Asterisk permet de transformer un tel PC en un autocommutateur PABX. Dans cette première étape, vous créerez un autocommutateur sur ce PC.

Pour cela :

- Vous installerez et configurerez Asterisk afin de prendre en charge les ports FXS.
- Vous attribuerez à votre autocommutateur le préfixe 0123 et vous numéroterez les ports FXS 1000, 1001, 1002, 1003, etc.
- Vous disposez de téléphones analogiques pour tester votre autocommutateur. Connectez vos téléphones et composez le numéro de téléphone depuis un téléphone vers un autre pour tester le bon fonctionnement de votre autocommutateur.
- Faites en sorte qu'il puisse y avoir affichage du numéro et transfert d'appel.

Création d'un d'un réseau téléphonique IP

Vous disposez d'un autre PC ne possédant pas de cartes dédiées à la téléphonie (pas de FXS ou FXO), simplement une carte réseau Ethernet. Il s'agit ici de réaliser un PBX entièrement basé sur IP. La téléphonie sur IP s'appuie sur le protocole SIP.

- Vous mettez en place le réseau 192.168.42.0/24 sur lequel vous connecterez votre PBX IP ainsi que deux autres PC.
- Vous créez des lignes SIP 2000, 2001, 2002, etc. que vous attribuerez aux téléphones IP. Vous utiliserez plusieurs types de téléphones IP : un téléphone IP filaire, un téléphone IP wifi, un softphone comme ekiga + casque et micro, un téléphone USB
- Connectez vos téléphones et composez le numéro de téléphone depuis un téléphone vers un autre pour tester le bon fonctionnement de votre autocommutateur IP.
- Faites en sorte qu'il puisse y avoir affichage du numéro et transfert d'appel.
- Mettez en place et expérimentez au maximum les services offerts par Asterisk : présentation du nom, filtrage d'appel, etc.

Création de la passerelle analogique

- Reliez votre PC commutateur analogique au réseau IP construit dans la section précédente.
- Faites en sorte que les téléphones IP puissent appeler les téléphones analogiques du réseau RTC et vice-versa.

b. Interconnexion de sites

Connexion IP à IP : Réalisez l'interconnexion entre les réseaux téléphoniques IP avec l'autre site.

Connexion RTC à RTC : A l'aide des ports FXO, réalisez l'interconnexion entre les réseaux analogiques des deux sites.

c. **Fonctionnalités supplémentaires**

- **Utilisation de proxy et de redirecteur pour la téléphonie IP** : Mettez en place un proxy et un redirecteur permettant l'enregistrement des numéros et (jabber) téléphone dans un intranet. Cette fonctionnalité est importante par rapport à l'évaluation finale du projet.
- **Intégration LDAP** : Vous déploierez et utiliserez un annuaire LDAP pour les services de présentation du nom, recherche numéro, etc.
- **Visio-conférence**: Sur votre machine Asterisk, prenez en compte le protocole H323 afin de permettre la visio-conférence. Testez.

Travail demandé

Vous répondrez à toutes les exigences demandées en déployant soigneusement votre plateforme téléphonique qui devra être fonctionnelle, maintenable et redéployable. Une attention particulière sera donnée à l'élaboration du rapport technique devant décrire les architectures manipulées, les pré-requis et les concepts notamment de téléphonie ainsi que les difficultés rencontrées, les remarques et les limitations. Le manuel d'installation et la description des configurations de logiciels seront quant à eux donnés en annexe.

2. <u>Supervision, métrologie et cartographie de réseaux (3 élèves)</u>
--

Tuteur : Tuyêt Trâm Dang Ngoc, dntt(à)u-cergy.fr

Une entreprise désire mettre en place un réseau composé des VLANs employé, DMZ et d'administration.

Le réseau de chaque site est composé d'un routeur matériel, gérant le routage inter-vlan ainsi que les filtres d'accès, et de commutateur(s) permettant de connecter les différents postes et serveurs. Ces derniers devront être placés sur le VLAN DMZ.

Les services à mettre en place sont les suivants :

- serveur DNS pour le domaine societe1.com.
- serveur Web www.societe1.com
- les services basés sur SSL suivants : HTTPS et adapter les ACL pour que ces services soient accessibles de l'extérieur.

La gestion des certificats devra être correctement réalisée. Ceci par :

- l'installation d'autorité(s) de certification
- la gestion de liste de révocation

a. **Listes de contrôle d'accès**

Une politique de sécurité doit être mise en œuvre sur le routeur gérant le routage inter-VLAN. Les listes de contrôle d'accès seront utilisées afin de :

- protéger le réseau interne des attaques venant de l'extérieur tout en autorisant l'accès aux services de la DMZ (DNS, Web)
- permettre aux utilisateurs d'accéder aux services extérieurs ;
- permettre l'accès interactif aux serveurs uniquement depuis les postes du service d'administration.
- tracer et/ou stocker les paquets répondant à certaines des règles que vous aurez établies.

b. **Surveillance du réseau**

Il est nécessaire de mettre en œuvre une station d'administration du réseau (NMS : Network Management Station) qui sera placée sur le VLAN DMZ. L'accès aux services offerts par cette NMS devra être restreint aux postes du service informatique et n'être accessibles que par https.

Les services de surveillance et de métrologie à mettre en place sont les suivants :

- *Nagios* : chargé de surveiller les équipements réseau ainsi que les services mis en œuvre ;
- *Cacti* : chargé de tenir à jour les graphes correspondant au trafic réseau sur les différentes interfaces des équipements ;
- *syslogd* : devra être configuré pour recevoir et stocker les alertes des équipements réseau (cf. commande logging des équipements).

Vous offrirez également les services suivants :

- surveillance de la charge CPU de chacun des serveurs (DNS, Web, mail) ;

- surveillance de l'imprimante
- mise en place d'un agent SNMP sur chacun des serveurs afin de maintenir les graphes de métrologie associés à ses interfaces réseau ;
- mise en place d'un plugin Nagios permettant d'interroger un agent SNMP et de détecter les dépassements de seuils liés à des OID spécifiques ;
- remontée des alertes par trappes SNMP vers la NMS (programme *snmptrapd*) qui devra être configuré pour alerter l'équipe informatique en cas de panne d'une interface physique sur laquelle est connectée un serveur).

Cartographie du réseau : Afin d'avoir une vision plus globale du réseau, vous installerez et configurerez un outil de cartographie du réseau (ex : *weathermap*)

c. Remontée d'alerte

Afin que les traces soient exploitables, facilités et priorités (et éventuellement la provenance) devront être pris en considération. Les politiques de rotation (ou d'archivage) des traces devront également être étudiées. Enfin, il sera nécessaire de bien identifier ce qui doit être tracé ou pas parmi les services, équipements et ACL que vous manipulez.

Suivant les cas, les traces seront simplement stockées dans un fichier, affichées sur la console, envoyées par mail à l'administrateur.

d. Recommandations

Vous prendrez soin d'expliquer le contexte, le détail de l'architecture, une synthèse des principes des techniques abordées, ainsi que les logiciels et matériels utilisés. Une réflexion devra être menée quant au passage de votre plateforme prototype vers un déploiement dans un environnement réel de production :

1. en termes de passage à l'échelle : avec beaucoup d'utilisateurs, d'équipement, de connexions, etc.
2. en termes de sécurité
3. en termes de facilité d'administration
4. en termes de fonctionnalités offertes
5. en termes de confort utilisateur

Vous justifierez tous vos choix.

Attention, les fichiers de configuration, les lignes de commandes, etc. doivent figurer en annexe et ne pas perturber la lecture du rapport. Ils ne doivent pas apparaître durant la présentation (sauf question du jury).

Pour les besoins de la démonstration, vous prendrez soin de préparer des scénarios pertinents montrant toutes les fonctionnalités que vous voudrez mettre en évidence. La démonstration devra être soigneusement préparée (machines démarrées, configuration réseau déjà initialisée, etc.).

3. Domaine Active Directory, contrôleur en lecture seule, DMZ, RADIUS, routeur et FTP (2-3 élèves)

Tuteur : Guillaume Renier, guillaume.renier(à)u-cergy.fr

Contexte

Une entreprise dispose d'un réseau local, d'une DMZ et est connectée à l'internet par l'intermédiaire d'un routeur. Un domaine AD est présent et configuré pour l'entreprise. Les contrôleurs sont accessibles uniquement sur le réseau local de l'entreprise. Chaque employé de l'entreprise dispose d'un compte sur le domaine AD.

Il est possible d'ouvrir des ports de la DMZ vers le réseau local (et donc les contrôleurs de l'AD).

Présentation

L'entreprise veut installer un serveur FTP dans la DMZ qui authentifiera les utilisateurs par l'intermédiaire de l'AD. Ce serveur doit créer dynamiquement un répertoire personnel pour chaque utilisateur.

Objectifs

Les contrôleurs AD 2008S peuvent être configurés en lecture seule. Les ouvertures de ports entre la DMZ et le réseau local ne se feront que vers un contrôleur 2008S en lecture seule. Le réseau local dispose donc d'au moins trois contrôleurs W2008S dont au moins 1 est en lecture seule et au moins 2 sont en lecture/écriture.

Le serveur FTP doit être un logiciel libre au sens large du terme. Il doit être installé sur un serveur UNIX (linux, FreeBSD, macOS...) et utiliser une authentification par PAM.

PAM doit être configuré pour utiliser :

- Soit un module pour RADIUS qui sera configuré pour utiliser un serveur RADIUS sur le serveur 2008.
- Soit un module LDAP qui sera configuré pour se connecter sur l'AD du serveur en lecture seule.

Le serveur FTP doit pouvoir être utilisé depuis l'internet et depuis le réseau local.

Les étudiants devront configurer 5 serveurs : 1 contrôleur 2008S en lecture/écriture, 1 contrôleur 2008S en lecture seule, 1 routeur (matériel ou logiciel) et un serveur UNIX. Le tout pouvant se faire sur des systèmes virtualisés.

Extension possible

La connexion sur le serveur FTP pourra se faire en SFTP ou en FTPS.

La connexion sur les répertoires personnels sur le serveur FTP pourra être accessible en NFS, CIFS depuis le réseau local.

4. Domaine Active Directory, VLAN, RADIUS, 802.1X, routeur, firewall, proxy filtrant (2-3 élèves)

Tuteur : Guillaume Renier, guillaume.renier(à)u-cergy.fr

Contexte

Une entreprise dispose d'un réseau local et est connecté à l'internet par l'intermédiaire d'un routeur / firewall. Un domaine AD est présent et configuré pour l'entreprise. Les contrôleurs sont accessibles uniquement sur le réseau local de l'entreprise. Chaque employé de l'entreprise dispose d'un compte sur le domaine AD.

Les employés sont soit des cadres, soit des non-cadres.

Présentation

L'entreprise souhaite accorder des droits d'accès à internet en fonction du statut (cadre / non cadre) des employés. Les cadres doivent disposer d'un accès complet à internet avec filtrage des sites web par liste noire. Les non cadres doivent disposer d'un accès à internet limité par liste blanche.

Pour cela, elle souhaite mettre en place une authentification 802.1X avec affectation dynamique de VLAN (il est possible d'imposer la marque du matériel actif utilisé.)

Le VLAN 3 sera réservé aux cadres et le VLAN 4 aux non-cadres.

Le VLAN 1 sera réservé à la gestion des switches.

Le VLAN 2 sera réservé aux serveurs.

Le routeur assurera du routage interVLAN (3--2 et 4--2). Les VLAN 3 et 4 seront cloisonnées.

Le filtrage des sites web se fera en fonction du VLAN : le routeur pourra rediriger de manière transparente les accès web (port 80) sur un proxy squid configuré pour utiliser des redirecteurs squidGuard (le filtrage des sites web ne se fait donc pas en fonction du nom utilisateur).

L'authentification 802.1X utilisera un serveur RADIUS qui authentifiera grâce à un annuaire LDAP.

L'annuaire LDAP sera au choix : l'AD des contrôleurs de domaine ou un OpenLDAP.

Néanmoins les comptes utilisateurs seront créés sur un AD.

Dans le cas d'un openLDAP il sera nécessaire de procéder à une réplication d'une partie de l'AD dans le LDAP (on pourra dans un premier temps utiliser un annuaire LDAP configuré spécifiquement).

Objectifs

Configurer l'ensemble des serveurs et des switches.

Configurer l'ensemble des routeurs / firewall, proxy (on pourra utiliser une distribution IP-COP).

Extension possible

On pourra faire en sorte que cette authentification fonctionne avec des postes Windows accrochées au domaine (avec donc une ouverture de session sur le domaine).

Sujets proposés à l'EPMI

5. Mise en place d'une infrastructure de sécurité de Haute disponibilité (2 élèves)

Tuteur Nabil Ouassini, n.ouassini(à)epmi.fr

En utilisant la technologie LVS sous linux vous devez mettre en place une infrastructure de sécurité sur laquelle repose un cluster de serveurs WEB.

A titre d'exemple vous installerez un ispcfg et PHP myadmin et prouverez que les modifications sont répercutées sur tous les serveurs de votre grappe et qu'il y a une continuité de service en désactivant un serveur du cluster.

Vous disposerez de 3 PC physiques DualCore pour émuler des serveurs de production.

Vous démontrerez que votre choix de type de LVS est le plus pertinent.

Vous devrez expliquer et documenter la technologie LVS Direct on donnant une comparaison entre un LVS Direct et LVS NAT.

6. Mise en place d'un cluster de calcul SERVEUR HPC (2 élèves)

Tuteur Nabil Ouassini, n.ouassini(à)epmi.fr

Mise en place d'un serveur de calcul sous 2008HPC.

La mise en place de cette technologie offre un environnement de travail où le client lance à partir de sa machine un calcul ou des simulations 3D et tout le rendu est calculé sur deux serveurs 2008 qui sont en cluster et gérés par un serveur Node (serveur HPC).

Vous disposerez de

- 2 serveurs Rack Dell octocore + un serveur tour
- 1 point d'accès WIFI
- 1 Switch
- 2 stations de travail.
- 1 logiciel Matlab.

7. Gestion intelligente de parc informatique (2 élèves)

Tuteur Nabil Ouassini, n.ouassini(à)epmi.fr

L'école dispose d'un grand réseau avec plusieurs VLAN. On nous demande de mettre en place la solution Pulse, qui est une architecture de gestion intelligente de parc informatique et qui permet d'administrer des parcs à partir de 2 postes. Avec cette technologie on veut recueillir les informations de chaque poste sur le réseau et agir sur les machines via une solution unique.

Pour éviter l'utilisation de la solution Mandriva, dont la plupart des services proposés sont payants, on installera PULSE2 sous Debian, qui est gratuit.

Vous aurez à votre disposition :

- Un serveur dual core
- Un switch pour créer des vlans,
- Une connexion internet,
- Un routeur pour émuler un serveur DHCP,
- 3 machines client pour tester.

8. Serveurs Web redondants (2 élèves)

Tuteur *Jean DOS SANTOS*, j.dossantos(à)epmi.fr

Mise en place de deux serveurs WEB (apache) redondants, avec un lien heartbeat et synchronisation des données avec Rsync, mais aussi avec une réplication de base de données en temps réel.

Les ressources utilisées sont deux serveurs Debian sur le même réseau avec l'application de réservation MRBS. Le lien heartbeat, Rsync et la réplication de base de données vont assurer la tolérance aux pannes et la continuité de service.

Tests à réaliser :

- Interruption du Serveur Principal pour voir si le Serveur Secondaire reprend le relais.
- Test avec l'analyseur de trames (Wireshark) pour détecter les 2 adresses physiques (2 serveurs) grâce à l'adresse virtuelle.